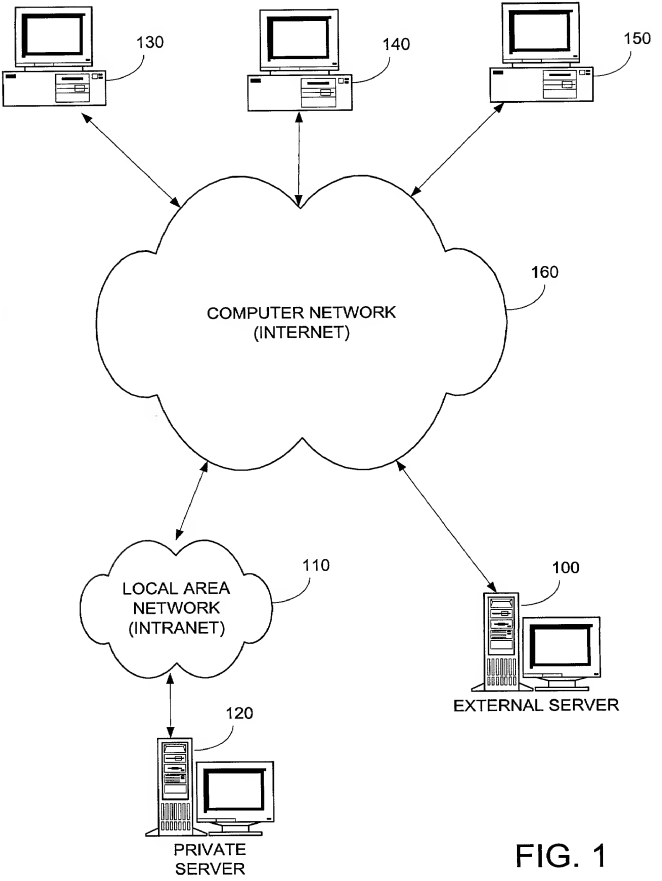
130
140
150
160
COMPUTER NETWORK
(INTERNET)
110
LOCAL AREA
NETWORK
(INTRANET)
100
EXTERNAL SERVER
120
PRIVATE
SERVER

FIG. 1

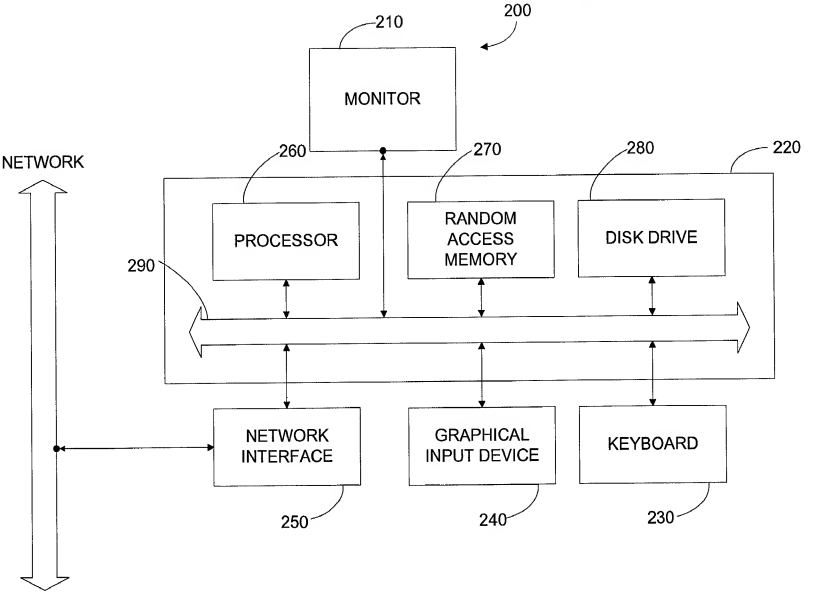
200
210
MONITOR
NETWORK
260
270
280
220
PROCESSOR
RANDOM ACCESS MEMORY
DISK DRIVE
290
NETWORK INTERFACE
GRAPHICAL INPUT DEVICE
KEYBOARD
250
240
230

FIG. 2

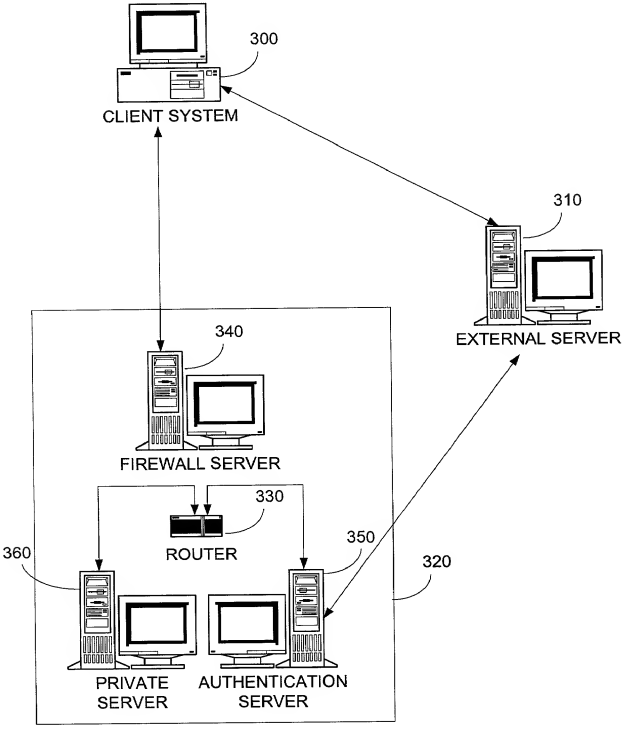
300
CLIENT SYSTEM
310
EXTERNAL SERVER
340
FIREWALL SERVER
330
ROUTER
350
360
320
PRIVATE SERVER
AUTHENTICATION SERVER

FIG. 3

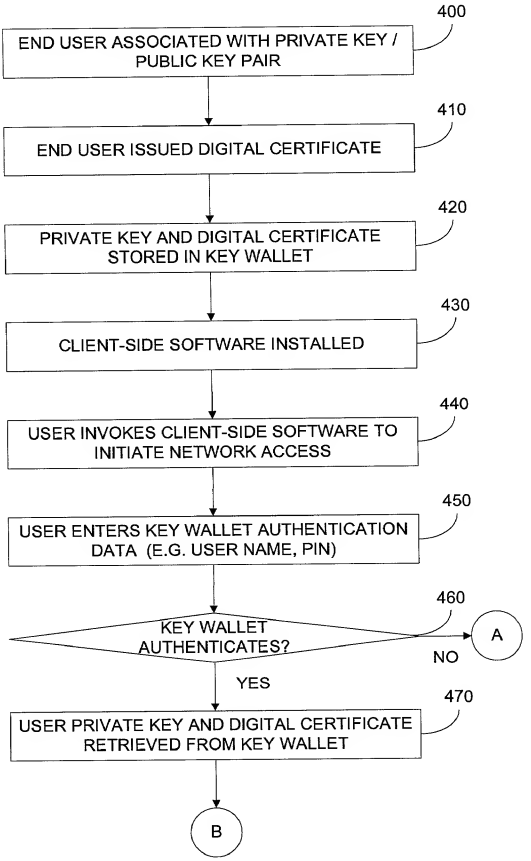
400
END USER ASSOCIATED WITH PRIVATE KEY / PUBLIC KEY PAIR
410
END USER ISSUED DIGITAL CERTIFICATE
420
PRIVATE KEY AND DIGITAL CERTIFICATE STORED IN KEY WALLET
430
CLIENT-SIDE SOFTWARE INSTALLED
440
USER INVOKES CLIENT-SIDE SOFTWARE TO INITIATE NETWORK ACCESS
450
USER ENTERS KEY WALLET AUTHENTICATION DATA (E.G. USER NAME, PIN)
460
KEY WALLET AUTHENTICATES?
A
NO
YES
470
USER PRIVATE KEY AND DIGITAL CERTIFICATE RETRIEVED FROM KEY WALLET
B

FIG. 4A

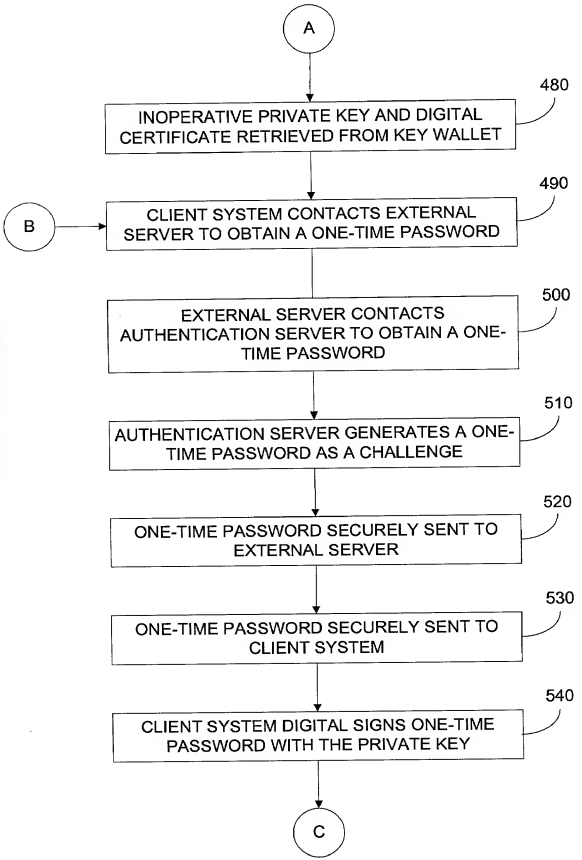
A
480
INOPERATIVE PRIVATE KEY AND DIGITAL CERTIFICATE RETRIEVED FROM KEY WALLET
490
B
CLIENT SYSTEM CONTACTS EXTERNAL SERVER TO OBTAIN A ONE-TIME PASSWORD
500
EXTERNAL SERVER CONTACTS AUTHENTICATION SERVER TO OBTAIN A ONE-TIME PASSWORD
510
AUTHENTICATION SERVER GENERATES A ONE-TIME PASSWORD AS A CHALLENGE
520
ONE-TIME PASSWORD SECURELY SENT TO EXTERNAL SERVER
530
ONE-TIME PASSWORD SECURELY SENT TO CLIENT SYSTEM
540
CLIENT SYSTEM DIGITAL SIGNS ONE-TIME PASSWORD WITH THE PRIVATE KEY
C

FIG. 4B

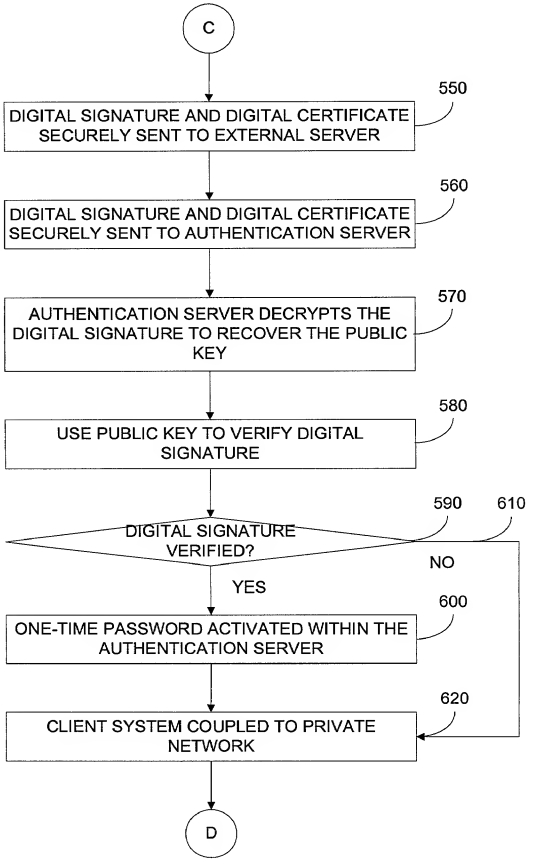
C
550
DIGITAL SIGNATURE AND DIGITAL CERTIFICATE SECURELY SENT TO EXTERNAL SERVER
560
DIGITAL SIGNATURE AND DIGITAL CERTIFICATE SECURELY SENT TO AUTHENTICATION SERVER
570
AUTHENTICATION SERVER DECRYPTS THE DIGITAL SIGNATURE TO RECOVER THE PUBLIC KEY
580
USE PUBLIC KEY TO VERIFY DIGITAL SIGNATURE
590
610
DIGITAL SIGNATURE VERIFIED?
NO
YES
600
ONE-TIME PASSWORD ACTIVATED WITHIN THE AUTHENTICATION SERVER
620
CLIENT SYSTEM COUPLED TO PRIVATE NETWORK
D

FIG. 4C

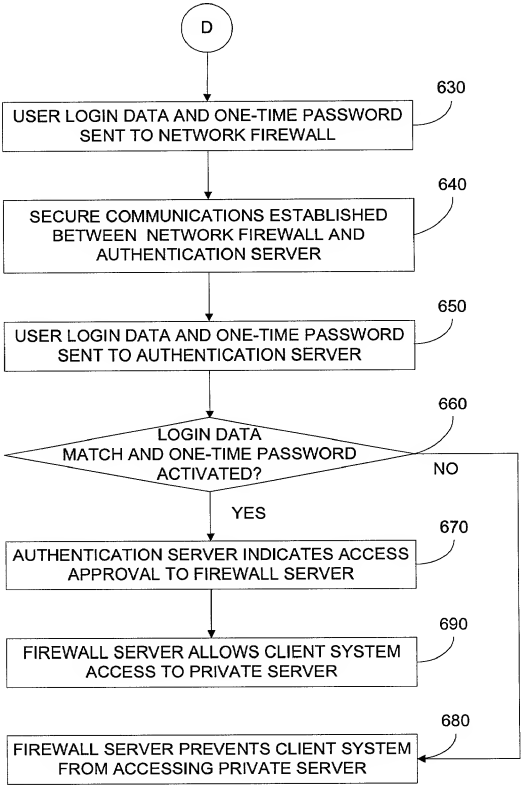
D
630
USER LOGIN DATA AND ONE-TIME PASSWORD SENT TO NETWORK FIREWALL
640
SECURE COMMUNICATIONS ESTABLISHED BETWEEN NETWORK FIREWALL AND AUTHENTICATION SERVER
650
USER LOGIN DATA AND ONE-TIME PASSWORD SENT TO AUTHENTICATION SERVER
660
LOGIN DATA MATCH AND ONE-TIME PASSWORD ACTIVATED?
NO
YES
670
AUTHENTICATION SERVER INDICATES ACCESS APPROVAL TO FIREWALL SERVER
690
FIREWALL SERVER ALLOWS CLIENT SYSTEM ACCESS TO PRIVATE SERVER
680
FIREWALL SERVER PREVENTS CLIENT SYSTEM FROM ACCESSING PRIVATE SERVER

FIG. 4D

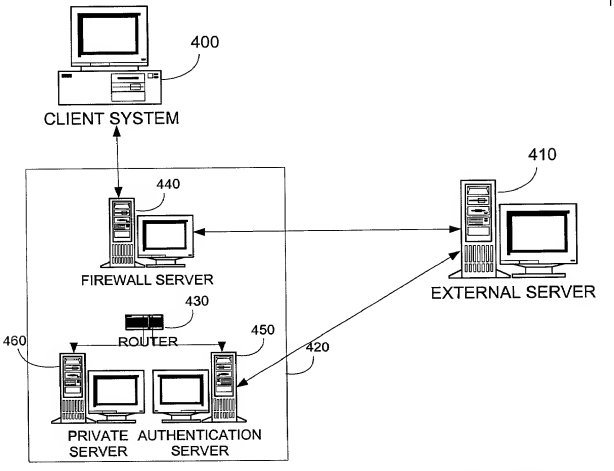
400
CLIENT SYSTEM
410
440
FIREWALL SERVER
EXTERNAL SERVER
430
ROUTER
460
450
420
PRIVATE SERVER
AUTHENTICATION SERVER

FIG. 5A

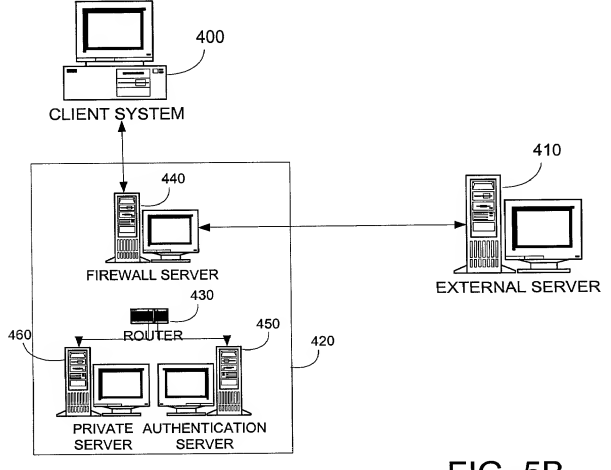
400
CLIENT SYSTEM
410
440
FIREWALL SERVER
EXTERNAL SERVER
430
ROUTER
460
450
420
PRIVATE SERVER
AUTHENTICATION SERVER

FIG. 5B